Resultat del control de qualitat del codi tipus; revisió sobre la implantació de les mesures de seguretat

El passat 28 de novembre de 2025 es va realitzar la sessió de control de qualitat del Codi Tipus de la Unió Catalana d'Hospitals per part de la consultora Faura-Casas assignada conjuntament amb el Sr. Javier Remacha, que és el delegat de protecció de dades de l'entitat Institut Guttmann (d'ara, endavant l'Entitat).

L'objectiu era fer seguiment de les àrees de millora i no conformitats de la darrera auditoria de protecció de dades, segons els requisits legals respecte a la protecció de dades de caràcter personal, establerts en el Reglament 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 referent a la protecció de les persones físiques pel que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant el RGPD) i, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de drets digitals, així com en el propi Codi Tipus de la Unió Catalana d'Hospitals. Així mateix, es revisen canvis que s'hagin pogut produir en l'entitat que tinguin impacte en aquesta matèria.

El resultat del control de qualitat es detalla en els següents apartats:

AUDITORIA

L'Entitat realitzà la darrera auditoria de protecció de dades el novembre de 2024. D'acord amb les informacions facilitades, els resultats de l'auditoria es van traslladar a la direcció de l'Entitat mitjançant la seva incorporació com a punt de l'ordre del dia, que va ser objecte de tractament en les reunions del Consell de Direcció dels mesos de gener i febrer de 2025, deixant-ne constància a les actes corresponents. Com a resultat d'aquestes sessions, s'ha elaborat un pla de millora, en el marc del qual s'han executat i tancat diverses actuacions, mentre que d'altres es troben en curs de desenvolupament.

REGISTRE D'ACTIVITATS DE TRACTAMENT (RAT)

S'ha revisat el registre d'activitats de tractament tenint en consideració els resultats de l'última auditoria. En concret, constatem que s'ha modificat el RAT per afegir-hi els tractaments de Usuaris del web Siidon, Canal de denúncies i Visitants de Guttmann Barcelona. Durant la reunió visualitzem el RAT i observem que ja inclou tots els apartats que requereix l'art. 30 RGPD.

Finalment, d'acord amb les informacions proporcionades, l'Entitat ha revisat la seva relació amb el Departament de Justícia, per al qual realitza el tractament de Treballadors en Benefici de la Comunitat (TBC) en qualitat d'encarregada del tractament. D'aquesta revisió se n'ha conclòs que, tot i no disposar actualment d'un contracte d'encàrrec de tractament amb entitats el Departament de Justícia, aquestes actuen com a responsables del tractament, mentre que l'Institut Guttmann hi intervé com a encarregat, tal com ja es feia constar al RAT. En aquest sentit, resta pendent promoure la signatura del corresponent contracte d'encarregat del tractament (CET).

MESURES DE SEGURETAT

Tal i com s'indicava en el darrer informe d'auditoria, la implementació de noves tecnologies en el tractament de dades de categoria especial (dades de salut, entre d'altres) implica en molts casos la necessitat de dur a terme avaluacions d'impacte. En particular, les tecnologies que podien requerir dur a terme avaluacions d'impacte i la seva actualització periòdica posterior, i que es van detectar durant els treballs de camp de la darrera auditoria, eren les següents:

- Ús de Medxat per a videoconsultala
- Implementació de la nova història clínica
- Sistema de reconeixement facial de pacients a Guttmann Barcelona
- Ús de l'empremta digital dels treballadors per al fitxatge i/o accés a espais restringits

D'acord amb les informacions facilitades, durant el darrer any s'ha dut a terme una activitat d'anàlisi de riscos i una avaluació d'impacte relativa a l'ús del sistema de gestió d'històries clíniques utilitzat per l'Entitat.

D'altra banda, s'informa que l'Entitat ha deixat d'utilitzar la dada biomètrica de l'empremta digital dels treballadors per a les finalitats de fitxatge i control d'accessos, la qual ha estat substituïda per un sistema d'identificació mitjançant targeta, de manera que ja no serà necessari la realització d'una avaluació d'impacte relativa a aquest tractament.

Finalment, resta pendent revisar la necessitat de dur a terme una avaluació d'impacte en la protecció de dades relativa a la implantació d'un sistema de reconeixement facial de pacients al centre Guttmann Barcelona, i la relativa a l'ús de Medxat per a videoconsultes.

ENCARREGATS DEL TRACTAMENT I PROVEÏDORS SENSE ACCÉS A DADES

Segons les informacions facilitades, l'Entitat ha elaborat un nou protocol de compres amb l'objectiu d'unificar i centralitzar els procediments d'adquisició que fins aleshores es realitzaven des de diferents àrees (comunicació, farmàcia, entre d'altres), mitjançant un procediment únic i homogeni. En aquest context, s'ha establert un procés d'homologació de proveïdors en el qual es tenen en consideració criteris diversos, com ara la sostenibilitat, l'economia circular, les acreditacions i certificacions de qualitat, així com els aspectes relatius a la protecció de dades, incloent-hi la subscripció d'un compromís de confidencialitat.

D'acord amb aquest protocol, tots els contractes són revisats pel departament jurídic de l'Entitat i, en el cas que durant aquesta revisió es detecti que la prestació del servei comporta el tractament de dades personals, es procedeix a la formalització del corresponent contracte d'encàrrec de tractament. Addicionalment, s'ha revisat el model de contracte d'encàrrec de tractament amb la finalitat de definir de manera més clara i detallada el servei prestat en cada supòsit.

Així mateix, s'informa que, en aquells casos en què existeixen contractes antics, formalitzats amb anterioritat a la implantació d'aquest protocol, l'Entitat procedeix a la seva revisió i actualització, corregint-ne el contingut i formalitzant, si escau, el corresponent contracte d'encàrrec de tractament. D'altra banda, segons s'indica, tots els proveïdors són sotmesos periòdicament a processos d'avaluació, amb la finalitat de verificar que es mantenen els requisits exigits en el procés de contractació.

Finalment, resta pendent confirmar si s'ha revisat el contracte d'encàrrec de tractament amb el proveïdor Zemsania tenint en compte les recomanacions de l'última auditoria, així com promoure la signatura del corresponent contractes d'encarregat del tractament (CET) amb el Departament de Justícia pel tractament de dades relatiu als treballadors en benefici de la comunitat (TBC).

LEGITIMACIÓ DE DADES

Respecte dels aspectes de millora que es detectaren sobre aquest punt en l'auditoria, es trasllada el següent:

- Personal – Segons s'ha esmentat abans, s'ha deixat d'utilitzar la dada biomètrica de l'empremta digital dels treballadors per a les finalitats de fitxatge i control d'accessos, la qual ha estat substituïda per un sistema d'identificació mitjançant targeta.

- Estudiants màster, residents i personal en pràctiques – S'ha modificat el procediment de recepció de candidatures, de manera que ja no s'accepten currículums per correu electrònic. Així, en cas que es rebi una candidatura per una via diferent a l'habilitada, com per correu electrònic, es respon als interessats indicant que la via habilitada per a la presentació de candidatures és l'apartat web «Treballa amb nosaltres». Un cop revisat aquest apartat web «Treballa amb nosaltres», constatem que les diferents ofertes ja inclouen una clàusula d'informació i acceptació de consentiment per al tractament de les seves dades personals amb finalitat de gestionar la candidatura concreta i d'incloure-les a una borsa de treball, per tal de que puguin ser tingudes en compte per futures candidatures. Aquesta clàusula d'informació i consentiment és correcta i ajustada als requisits de l'RGPD.

- Comunicació – S'ha elaborat un model de document específic per a la recollida del consentiment dels treballadors per a l'ús de la seva imatge amb finalitats de comunicació, el qual actualment és gestionat pel departament de Comunicació. Així, anteriorment, el consentiment es recollia de manera genèrica en el moment de la incorporació del treballador, mitjançant una autorització d'ús de la imatge amb caràcter indefinit. Aquest enfocament ha estat substituït per un sistema de consentiments diferenciats i vinculats a finalitats concretes, de manera que, per a cada publicació o esdeveniment específic, com ara la gravació d'un vídeo commemoratiu del 60è aniversari de l'Entitat, es recull un consentiment específic, limitat a aquesta finalitat. Queda pendent revisar si aquest document ja informa de totes les xarxes on es penjaran i de les possibles transferències internacionals de dades que pot suposar l'ús de xarxes socials com Facebook.

- Guttmann Barcelona Life i Sports & Life Guttman – S'ha revisat el formulari del web previst per al procediment de recollida de dades de Guttmann Barcelona Life i Sports & Life Guttman, de manera que ja informa correctament sobre la informació de l'art. 13 RGPD sobre aquest tractament de les dades.

  Videovigilància – Segons s'indica, s'ha reduït el temps de conservació de les imatges de les càmeres de videovigilància a 30 dies, tal com preveu la Guia de Videovigilància de l'Agència Espanyola de Protecció de Dades (AEPD).
- Visitants de Guttmann Barcelona – s'ha instal·lat un cartell informatiu al centre amb la finalitat de facilitar tota la informació relativa al tractament de les seves dades personals. A més, segons s'informa, ja no es recull la dada del DNI, limitant-se el registre a la recollida del nom i de l'hora d'entrada i sortida. Resta pendent revisar aquest procediment de recollida de dades per al registre, atès que, segons les informacions facilitades, no totes les visites passen per recepció en el moment de comunicar la seva sortida, fet que pot afectar la integritat i l'exactitud del registre.

  Investigació: Resta pendent treballar per fer signar al personal investigador un document de compromís que reculli l'obligació de confidencialitat i la prohibició de dur a terme qualsevol intent de reidentificació de les persones objecte dels estudis de recerca.
- BBHI - Barcelona Brain Health Initiative: Segons s'indica, aquest tractament feia referencia a un projecte de recerca específic que ja ha finalitzat, de manera que aquest no és un tractament que s'estigui duent a terme actualment a l'Entitat.

- Empremtes digitals àrea mèdica: Segons les informacions proporcionades, a l'Entitat s'ha deixat d'utilitzar la dada biomètrica de l'empremta digital per identificar els pacients, de manera que aquest ja no és un tractament que s'estigui duent a terme actualment a l'Entitat.

- Canal de denúncies – Resta pendent incloure al Canal de denúncies un procediment que permet informar als usuaris de la informació de l'art. 13 RGPD sobre el tractament de les seves dades.

DRETS DE LES PERSONES INTERESSADES

S'indica que s'ha creat una base de dades específica en la qual es registren tots els exercicis formals dels drets d'accés, rectificació, supressió, oposició, limitació i portabilitat (ARSOPOL). A més, segons s'informa, a través del sistema de gestió de la història clínica es disposa d'un registre de canvis que permet traçar les modificacions efectuades. D'altra banda, les sol·licituds de rectificació de dades es gestionen directament mitjançant el programa Access.

No obstant, durant la reunió de checklist no es revisa aquest registre, de manera que no es pot constatar que les sol·licituds de dret es resolguin en el degut temps i forma. És important que les sol·licituds es resolguin en temps i forma, i que es guardi evidència.

Finalment, s'informa que al centre de Guttmann Barcelona s'ha revisat el procediment de presentació de sol·licitud de drets ARSOPOL de manera que ja no es requereix la recollida del DNI als interessats per defecte quan sigui possible identificació de la persona sol·licitant per mitjans menys invasius.

REGISTRE D'INCIDÈNCIES I NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

S'ha incorporat en el Manual de bones pràctiques, el qual s'entrega tant al nou personal laboral, com als estudiants en pràctiques i als treballadors autònoms contractats per prestar algun servei a l'Entitat, indicacions específiques en relació a la obligació de notificar al DPD qualsevol possible incidència de seguretat en la protecció de dades de que siguin coneixedors. A més, segons les informacions proporcionades, també es donen indicacions al respecte mitjançant la formació online sobre protecció de dades que han de cursar totes les noves incorporacions.

En aquest context, s'informa d'un incident de seguretat ocorregut recentment, consistent en el segrest del compte corporatiu d'Instagram. Un cop detectada la incidència, es va informar inicialment el responsable de Seguretat i la Direcció d'Informàtica, i posteriorment el Delegat de Protecció de Dades i la Direcció de l'Entitat, i es va comunicar a la *Agencia Española de Protección de Datos* (AEPD) en el termini de 30 dies. Segons s'informa, l'incident no va afectar dades de pacients.

DIFUSIÓ DE FUNCIONS I OBLIGACIONS

S'ha elaborat i implementat un pla de formació anual en matèria de protecció de dades, de caràcter obligatori, que es realitza en el moment de la incorporació del personal i es renova amb periodicitat anual. Segons s'indica, aquesta formació no ha estat completada pel 100 % de la plantilla, però sí per un percentatge aproximat del 85–90 %, i es disposa d'un registre de les persones que l'han realitzada.

Addicionalment, s'ha impartit una formació específica en matèria de ciberseguretat, que ha estat realitzada per la totalitat del personal. Aquesta formació està prevista també per a les noves incorporacions i resta pendent determinar la periodicitat amb què es durà a terme la seva actualització o reforç. En tots els casos, l'Entitat manté un registre de participació en aquestes accions formatives.

Queda pendent incloure en el protocol de bones pràctiques instruccions o una prohibició sobre fer fotos i gravacions al centre, llevat autorització en contrari.

MESURES DE SEGURETAT TÈCNICA I ORGANITZATIVA

S'informa que s'està treballant en les mesures de seguretat informàtica. Sobre les àrees de millora detectades en l'informe de l'auditoria, se'n descriu la situació corresponent:

- INFORMÀTIQUES

- Accessos remots: Pel que fa als accessos remots mitjançant VPN, s'ha implantat un sistema d'autenticació reforçada amb doble factor. En concret, s'utilitza l'aplicació Microsoft Authenticator, que sol·licita la doble autenticació de manera periòdica, així com en determinades circumstàncies, com ara el canvi de contrasenya o l'inici de sessió des d'un dispositiu diferent.
- Registre d'accessos informàtics: S'ha implementat un procediment de revisió periòdica, consistents en la selecció aleatòria d'un pacient cada 2 o 3 mesos aproximadament. No obstant, resta pendent la formalització d'aquest procés mitjançant l'elaboració d'un procediment específic per escrit que reguli de manera sistemàtica la revisió i documentació dels registres d'accés. Aquest procediment hauria d'incloure, entre d'altres, la definició del nombre d'històries clíniques a revisar en cada període, els criteris de selecció dels casos (ja sigui de manera aleatòria o atenent perfils de major risc, com ara pacients VIP o personal de la pròpia Entitat) i l'obligació de documentar els resultats de les revisions mitjançant els corresponents informes de control.
- Sortida de dades: Segons les informacions facilitades, l'Entitat es troba actualment revisant el sistema d'encriptació dels correus electrònics que contenen dades personals. Fins ara, el procediment habitual consistia en l'enviament de l'arxiu encriptat i la comunicació posterior de la contrasenya per una via separada. Amb la finalitat de millorar la seguretat, s'està valorant la substitució d'aquest sistema per mecanismes alternatius, com ara l'enviament mitjançant una plataforma corporativa o, en determinats casos, la comunicació telefònica, amb l'objectiu de deixar d'utilitzar progressivament el sistema dels dos correus electrònics.

  Pel que fa a la comunicació d'aquestes mesures al personal, s'han impartit formacions específiques i s'han facilitat instruccions puntuals per correu electrònic, mentre que el Manual de bones pràctiques recull actualment les indicacions vigents. Un cop es formalitzi el nou procediment d'enviament segur de dades i encriptació, aquestes qüestions hauran de quedar degudament regulades per escrit i s'hauran de donar indicacions clares al personal de l'Entitat.

- FÍSIQUES

- Criteris d'arxiu: Segons les informacions facilitades, l'Entitat ha avançat de manera significativa en la reducció de la documentació en suport paper, procedint a la seva destrucció progressiva un cop digitalitzada la informació considerada rellevant. Actualment, la generació de nova documentació es realitza majoritàriament en format digital, mitjançant canals web i arxius en format PDF, de manera que pràcticament no es genera nova documentació en paper. Segons s'informa, no es conserva documentació amb una antiguitat superior als deu anys. No obstant, encara manca establir i documentar per escrit uns criteris d'arxiu i destrucció de la documentació més antiga i innecessària que ja no caldria continuar conservant, alhora que permeti garantir el ple exercici dels drets dels interessats.

Altres aspectes que van sortir a la reunió de *checklist* són:

- Recentment l'Entitat ha aprovat el nou Pla Estratègic del Grup per al període 2026–2027, que preveu la implementació de diversos canvis rellevants en l'organització. En aquest context, està prevista la celebració d'una propera reunió del Patronat en la qual s'ha de sotmetre a aprovació un canvi en la imatge de marca del Grup. Aquests processos de transformació estratègica i corporativa comportaran previsiblement la necessitat de revisar i actualitzar determinats aspectes organitzatius i documentació interna en els propers mesos.

- Addicionalment, segons s'indica, recentment s'ha actualitzat la política de contrasenyes, incrementant-ne el requisit mínim de longitud de vuit a deu caràcters i establint l'obligatorietat d'incloure caràcters alfanumèrics i símbols. Així mateix, s'ha fixat l'obligació de renovar la contrasenya amb una periodicitat trimestral i s'ha restringit la reutilització de les darreres vint-i-quatre contrasenyes.

  Finalment, l'Entitat es troba en procés de certificació en l'Esquema Nacional de Seguretat (ENS) de nivell bàsic. Segons s'indica, a data actual el grau de compliment se situa lleugerament per sobre del 70 %, amb l'objectiu d'assolir aproximadament el 75 % abans de finalitzar l'any en curs i arribar a un nivell de compliment proper al 90 % durant l'any vinent. Aquest procés implica la implantació progressiva de noves mesures tècniques i organitzatives de seguretat que reforçaran el nivell de protecció ja existent a l'Entitat.

Les àrees que encara estan pendents de treballar són: realitzar les anàlisis de riscos i les avaluacions d'impacte que queden pendents, promoure la signatura dels contractes d'encarregat del tractament (CET) amb el Departament de Justícia, per al qual realitza el tractament de Treballadors en Benefici de la Comunitat (TBC) en qualitat d'encarregada del tractament, , confirmar si s'ha revisat el contracte d'encàrrec de tractament amb el proveïdor Zemsania tenint en compte les recomanacions de l'última auditoria, revisar si el document d'obtenció del consentiment dels treballadors per a l'ús de la seva imatge amb finalitats de comunicació document ja informa de totes les xarxes on es penjaran i de les possibles transferències internacionals de dades que pot suposar l'ús de xarxes socials com Facebook, revisar el procediment de recollida de dades per al registre de visitants de Guttmann Barcelona, atès que, segons les informacions facilitades, no totes les visites passen per recepció en el moment de comunicar la seva sortida, incloure al Canal de denúncies un procediment que permeti proporcionar als usuaris la informació de l'art. 13 RGPD sobre el tractament de les seves dades, revisar que les sol·licituds de drets ARSOPOL es responen en temps i forma i es manté una evidència documental, incloure en el protocol de bones pràctiques indicacions sobre fer fotos i gravacions al centre, elaborar d'un procediment específic per escrit que reguli de manera sistemàtica la revisió i documentació dels registres d'accessos a les històries clíniques, i establir per escrit uns criteris d'arxiu i destrucció de la documentació més antiga i innecessària que ja no caldria continuar conservant i que permetin garanteixi el ple exercici dels drets dels interessats.

Barcelona, 29 de desembre de 2025.

39334508T PERE RUIZ (R: B58671710)

Firmado digitalmente por 39334508T PERE RUIZ (R: B58671710)
Fecha: 2025.12.29 13:25:44 +01'00'

Pere Ruiz Espinós

Soci